ALSD Local 106 (Rev. 07/13) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Alabama

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

information associated with [redacted]t@icloud.com and [redacted]t@icloud.com that is stored at premises controlled by Apple Inc.

Case No. 23-MJ- 126-B

Filed Under Seal

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 846, 841(a)(1); 18 U.S.C. §§ 924(c)(1)(A)(i), 922(g)(1); 26 U.S.C. § 5861(d)	Conspiracy to PWID marijuana, PWID marijuana, possession of a firearm in furtherance of a drug trafficking crime, possession of a firearm by a prohibited person (felon), possession of an unregistered firearm

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Kimberly Suhi
Applicant's signature

Kim Suhi, Senior Special Agent, ATF
Printed name and title

Sworn to before me and attestation acknowledged pursuant to FRCP 4.1(b)(2).

Date: May 19, 2023

Sonja F. Bivins
Judge's signature

City and state: Mobile, Alabama

Sonja F. Bivins, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ALABAMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [redacted]@icloud.com AND [redacted]@icloud.com THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	**Case No. 23-MJ- 126-B** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Senior Special Agent Kimberly A. Suhi, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Senior Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (hereinafter "ATF"), and have been since 2003, approximately 19 years. My

responsibilities included investigating and enforcing the federal firearms laws. I attended the Criminal Investigator Training Program at the Federal law Enforcement Training Center (hereinafter "FLETC"), in Glynco, Georgia, for approximately 10 weeks in 2003, where I received training and instruction as a Special Agent, including firearms training, the execution of search and arrest warrants, investigative techniques and legal instruction, which covered Fourth Amendment searches and seizures. Subsequently, for approximately 14 weeks in 2003, I attended specialized training known as New Professional Training through ATF at FLETC, where I received instruction in firearms technology and identification, firearms trafficking, explosives, and arsons. During my career as a Special Agent, I have testified on several occasions in grand jury proceedings, where my testimony has contributed to the indictment of numerous individuals; have obtained numerous federal search warrants; have been involved with the execution of state and federal search and seizure warrants, where firearms, firearms parts and accessories, ammunition, controlled substances, drug paraphernalia, electronic devices, electronic parts and accessories and the data within those electronic devices and accessories have been seized; and, I have participated in numerous arrests of individuals charged with federal and/or state firearms and narcotics violations.

3. In addition to investigating federal firearm violations, I also investigate criminal and civil violations of the Controlled Substances Act. In connection with my official duties and responsibilities as a federal law enforcement officer, I have experience in the debriefing of defendants, witnesses, confidential sources, and other persons who have knowledge of the distribution and transportation of controlled substances and the laundering and concealing of proceeds from drug trafficking, which is similar to how firearms traffickers operate. I am familiar

with firearms and narcotics traffickers' methods of operation, including, but not limited to, the distribution, storage, and transportation of narcotics and firearms, as well as the collection and laundering of money representing the proceeds of firearms and narcotics trafficking. Based upon my training and experience, I know that:

- Firearms and narcotics traffickers maintain on hand at their residences' large amounts of United States currency in order to maintain and finance their ongoing narcotics business and/or which represent proceeds generated from the distribution of narcotics and sale of firearms.

- Firearms and narcotics traffickers maintain books, records, receipts, notes, ledgers, airline tickets, money orders, and other documents relating to the transportation, ordering, sale and distribution of controlled substances, which are usually maintained where the traffickers have ready access to them.

- When firearms and narcotics traffickers amass proceeds from their illegal sales, the traffickers attempt to legitimize these profits, and to accomplish these goals, traffickers often rely on domestic banks and their services, Western Union wire transfers, securities, cashiers' checks, money drafts, letters of credit, brokerage houses, real estate, shell corporations, and business fronts.

- Firearm and narcotics traffickers commonly maintain addresses or telephone numbers in books and documents which list names, addresses and/or telephone numbers of their associates in the trafficking organization; such records are normally maintained at the traffickers' residences, businesses and other locations under their control.

- Firearms and narcotics traffickers take or cause to be taken photographs and videos of themselves, their associates, their property, and the illegal firearms and narcotics they sale, and often maintain these photographs and videos in their residences and/or other locations under their control.

- Courts have recognized that evidence of unexplained wealth, including jewelry and extensive travel, may be probative evidence of crimes motivated by greed, including crimes relating to the illegal trafficking in controlled substances and the sale of firearms.

- Firearms and narcotics traffickers commonly use cellular telephones and other electronic devices in order to communicate with their criminal associates and those devices are commonly carried with them or kept at locations under their custody and control, such as their residences and vehicles, and contain names, numbers and other information stored in the devices.

4. Based on my training and experience, I am familiar with the methods and practices used by individuals and organizations involved in illicit activities that generate large amounts of income. These methods include cash purchases, the purchasing of numerous monetary instruments with cash in amounts less than $10,000, the use of aliases and nominees, the use of businesses as "fronts" in an attempt to legitimize and conceal their activities and profits, and the use of "off-shore" banking in an attempt to break the paper trail. These and other schemes are commonly referred to as "money laundering."

5. During the course of my training and experience and through conversations with other more experienced law enforcement officers, I have learned of various methods used by firearms and narcotics traffickers, as well as mere possessors of illegal firearms and accessories, to conceal their assets, income, and activities from the government and other third parties. Based on my training and experience, and through conversations with other officers and agents, I know the following:

- Traffickers often utilize electronic devices and social media platforms/applications to facilitate communication with co-conspirators and/or store contact information (i.e., names, telephone numbers, physical address, e-mail address, usernames, etc.) of associates.

- Traffickers often utilize multiple electronic devices and/or social media platforms/applications in an effort to compartmentalize their firearms and narcotics trafficking businesses. Multiple electronic devices and/or social media platforms/applications are often utilized in an effort to maintain anonymity and independent contact between sources of supply and a range of customers.

- Traffickers maintain records, receipts, notes, ledgers, and other items relating to the transportation, ordering, sale and distribution of firearms and controlled substances, which are usually maintained where the traffickers have ready access to them, and which are often stored on digital media or an iCloud type service.

- Traffickers commonly maintain identifying information in electronic devices which list names, telephone numbers, physical address, e-mail address, and usernames of their various associates in the trafficking organization; such records are normally maintained within places/things under their control.

- Traffickers take or cause to be taken photographs and videos of themselves, their associates, their property, and the illegal firearms, firearms parts and accessories and narcotics they distribute, and often maintain these photographs within places/things under their control, including on electronic devices or an iCloud type service.

- Traffickers commonly use electronic devices in order to communicate with their criminal associates and those electronic devices are commonly carried with them or kept at locations under their custody and control, such as their residences and vehicles, and contain names, telephone numbers, physical address, e-mail address, usernames and other information stored in the electronic devices.

- Traffickers commonly are involved in money laundering and retain records of their transactions within places/things under their control. Records of this kind are also often stored within electronic devices, digital media or an iCloud type service.

6. I also have extensive experience in debriefing defendants, participant witnesses, informants, and other persons who have had personal experience and knowledge of the amassing, spending, converting, transporting, distributing, and concealing the proceeds from illegal activities.

7. From my background, I know that individuals engaged in firearms trafficking, drug trafficking and/or money laundering frequently retain records of their transactions within their residence, place of business, rented storage units, vehicles, or other places under their control. These records may be in the form of written notes and correspondence, receipts, negotiated

instruments, loans, bank statements, and other records. Records of this kind are also often stored in electronic devices, on digital media or in an iCloud type service.

8. Individuals who amass proceeds from illegal activities routinely attempt to further that conduct and/or conceal the existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, money drafts, traveler's checks, wire transfers, etc. Records of such instruments are routinely maintained at the individual's residence or place of business.

9. I also have extensive experience in the identification and handling of parts and accessories that convert a semi-automatic firearm into a machinegun. The National Firearms Act ("NFA"), defines machinegun as "any weapon which shoots, is designed to shoot, or can be readily restored to shot, automatically more than one shot, without manual reloading, by a single function of the trigger. The term shall also include the frame or receiver of any such weapon, **any part designed and intended solely and exclusively, or combination of parts designed and intended for use in converting a weapon into a machinegun**, and any combination of parts from which a machinegun can be assembled if such parts are in the possession or under the control of a person." 26 U.S.C. § 5845(b) (emphasis added). I have identified and handled numerous Glock "switches," which are devices designed and intended to convert a semi-automatic firearm, a Glock-type pistol, into a machinegun. The extend leg from the Glock switch is designed to push the trigger bar down and out of engagement with the firing pin as the slide closed, releasing the partially retracted firing pin to travel forward and fire a cartridge. When the trigger is depressed, this device enables a

Glock-type pistol to shoot automatically more than one shot, without manual reloading, by a single function of the trigger.

10. The National Firearms Registration and Transfer Record ("NFRTR") is the central registry of all NFA firearms in the United States, which are not in the possession or under the control of the United States Government. The registry includes (1) the identification of the firearm, (2) date of registration, and (3) identification and address of the person entitled to possession of the firearm (the person to whom the firearm is registered). A Glock Switch alone or attached to a Glock-type firearm would have to be registered with NFRTR to be possessed legally.

11. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. All dates, locations, and amounts referenced in my affidavit are approximations.

12. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute Marijuana); 21 U.S.C. § 841(a)(1) (Possession with Intent to Distribute Marijuana); 18 U.S.C. § 924(c)(1)(A)(i) (Possession of Firearm in Furtherance of a Drug Trafficking Crime); 18 U.S.C. § 922(g)(1) (Possession of a Firearm by a Prohibited Person (Felon)); and 26 U.S.C. § 5861(d) (Possession of an Unregistered Firearm) have been committed by **Hassan Decalpton JONES** (hereinafter referred to as "**JONES**"). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

13. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the United States District Court for the Southern District of Alabama is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

14. On January 26, 2023, Mobile Police Department (hereinafter referred to as "MPD") Detective Charles Hunter obtained a search warrant from a Mobile County District Judge to search **JONES's** apartment on Shelton Beach Road in Eight Mile, Alabama. In the affidavit supporting the search warrant, Det. Hunter detailed a surveilled controlled purchase of marijuana that a confidential informant made from **JONES** on Omega Avenue in Mobile, Alabama, just after **JONES** left his apartment on Shelton Beach Road. At the time of the controlled purchase of marijuana from **JONES**, the confidential informant observed a firearm on **JONES**'s person.

15. On February 1, 2023, an MPD SWAT team and narcotics detectives executed the search warrant at **JONES's** apartment on Shelton Beach Road. Police detained Rickey Edwards walking away from the apartment. Police then breached the front door of the apartment and called all occupants out of the apartment. Police observed **JONES** running into the second bedroom on the left, but he later exited the apartment.

16. In the second bedroom on the left, in the same room police observed **JONES** running into, detectives located two firearms, ammunition, cellular telephones, and narcotics. The firearms are described as a (1) Glock, Model 22Gen5, .40 caliber pistol, bearing serial number

BMLC248, with an extended magazine loaded with twenty-two (22) .40 caliber rounds of ammunition; and a (2) Glock, Model 23, .40 caliber pistol, bearing serial number BWBT082, equipped with a machinegun-conversion device (*i.e.*, a "Glock switch") and an extended magazine loaded with fourteen (14) .40 caliber rounds of ammunition. Inside a vehicle belonging to [redacted] a [redacted], detectives located four pounds of marijuana.

17. [redacted] was interviewed by Det. Hunter. She stated that she stayed in the second bedroom on the left with **JONES**. She stated she was unaware of anything illegal inside the bedroom. She confirmed that the vehicle from which detectives seized four pounds of marijuana belonged to her and that she drove the vehicle, but stated **JONES** was the last person to drive the vehicle.

18. Det. Hunter also interviewed [redacted] Det. Hunter advised [redacted] of his *Miranda* rights and asked if he understood them. [redacted] waived his rights and agreed to speak with Det. Hunter. [redacted] claimed **JONES** as an occupant of the apartment and stated that he frequented the apartment, but he did not live at the apartment full time. [redacted] claimed he did not know about the firearms and narcotics located inside the apartment.

19. ATF queried the NFRTR and confirmed that **JONES** had never had a machinegun registered to him at any time, including on February 1, 2023.

20. In connection with the February 2023 incident, I seized and searched **JONES's** iPhones pursuant to a search warrant. The phones contain hundreds of pictures, videos, text messages, and other data relating to **JONES's** possession of narcotics and firearms. I have provided a non-exhaustive sample of such data below. The phones also are linked to the Apple IDs

that are the subject of this warrant application—*i.e.*, [redacted]**icloud.com** and [redacted]**@icloud.com**, which appear to be **JONES's** Apple IDs based on my review of the data on the phones.

21. For example, on one of **JONES's** iPhones, I found and viewed several pictures of what appears to be bulk marijuana with metadata dated between November 5, 2022, and December 23, 2022 (*see, e.g.*, Figure 1 below), and a video of what appears to be codeine syrup with a label in **JONES's** name with metadata dated January 25, 2023 (*see, e.g.*, Figure 2 below). The phone also contains a photo screenshot, with metadata dated January 23, 2023, of a news article regarding a federal firearms prosecution of [redacted] in the Southern District of Alabama involving a "Glock switch," demonstrating **JONES's** knowledge (*see* Figure 3 below).

Fig. 1 (photo of apparent bulk marijuana, dated Nov. 5, 2022).

Fig. 2 (screenshot of video of apparent codeine syrup, dated Jan. 25, 2023).

SEALED

Fig. 3 (screenshot of news article reporting on "Glock switch" prosecution in the Southern District of Alabama).

22. On **JONES's** other iPhone, I found and viewed several text message strings, dated between July 2021 and January 2023, discussing apparent drug transactions. For example, on

July 31, 2021, **JONES's** iPhone texted someone using phone number x1655, "I got 3 perks left." Based on my training and experience, I know that "perk" is a reference to Percocet pills. The person using number x1655 responded, "Sell me perk." **JONES's** iPhone replied, "My brother got them how many u want." The person using number x1655 responded, "One em n I thought u had dem tabs?" Based on my training and experience, I know that "tabs" is a reference to Lortab pills. On August 1, 2021, **JONES's** iPhone replied, "They gone." Later, on November 19, 2021, **JONES's** iPhone wrote, "What it do lol bra I got them zips 115 real smoke fwm." Based on my training and experience, I know that "zips" is a reference to ounces of drugs, and "smoke" is a reference to marijuana.

23. In another example, on November 21, 2021, a contact using phone number x1228 texted **JONES's** iPhone, "How u gone do me this time plug I told u I'm only fuckin with u on this weed tip u my plug." Based on my training and experience, I know that "plug" is a reference to a source of supply for drugs, and "weed" is a reference to marijuana. **JONES's** iPhone responded, "What u had besides the 70." The person using number x1228 replied, "I just got 9 grams I'm tryna turn up ima get this shit gone I'm do u right."

24. In another example, on June 20, 2022, a contact using phone number x4115 texted **JONES's** iPhone, "Brudda when you called it was too much going on my people spot got hit this morning & shit been slow I sold my bag but the one you fronted me I sold a Qp out of it, ion want you think a nigga playing cause we both bout our money I was gone come to you when these other 12 zips gone." The contact then sent an image depicting 12 apparent ounce-sized bags of marijuana. Based on my training and experience, I know that "Qp" is a reference to a quarter of a pound of drugs, and "12 zips" is a reference to 12 ounces of drugs. **JONES's** iPhone responded,

"Gotta come on with it bra my ppl waitin on money." On June 22, 2022, **JONES's** iPhone followed up, "U got bring that money today homes shit been a week."

25. In another example, between July 10, 2022, and August 27, 2022, **JONES's** iPhone exchanged numerous text messages with a contact using a (310) area code number (Los Angeles, California). The messages appeared to relate to apparent shipments of packages from California—a known source of supply for bulk marijuana—to Alabama. The messages also discussed tracking of those shipments and payments for the same via Cash App.

26. In another example, on August 7, 2022, a contact using phone number x5506 texted **JONES's** iPhone, "U got me zip for 750$." Later, on August 30, 2022, the person using phone number x5506 wrote, "U got a quarter of soft." Based on my training and experience, I know that "soft" is a reference to cocaine. **JONES's** iPhone responded, "Wya," which means "where you at." **JONES's** iPhone then exchanged messages with the person using phone number x5506 regarding meeting up.

27. In another example, on January 30, 2023—two days before the search warrant at **JONES's** apartment—a contact using phone number x2181 texted **JONES's** iPhone, "You said we can work that shit off on the back end If I swear start fwu! We way better than that, yeen never had another nigga text my phone, I'm yo lil brudda, I fell back fr cause you was giving me good weed at first & start serving me bs If we gone lock back in I need to know ain't nobody on no bs cause we get money Nigga Ian trynna have us on no bs can't trusting each other." Based on my training and experience, I believe these messages relate to a conspiracy to distribute marijuana for profit. On January 31, 2023—the day before the search warrant at **JONES's** apartment—**JONES's** iPhone responded, "I been told u it's all good fool u bs." The person using number

x2181 replied, "Fasho brudda & the prices still the same or lil lower cause Ima be getting 2 a week this time starting next week cause I just got 2 yesterday."

28. **JONES's** iPhone also contains several entries in the "Notes" app of what appear to be drug ledgers. For example, on March 20, 2022, **JONES's** iPhone contains an entry listing several apparent names or nicknames of individuals next to what appear to be amounts owed, ranging from "50" to "450." There are other similar apparent drug ledgers in the phone.

29. The "Notes" app of **JONES's** iPhone also contains apparent rap lyrics referencing "Glock switches." For example, on June 3, 2022, one entry states, "Got the Glock with the dick n how I shoot ion need a switch." **JONES** has been depicted in rap videos posted publicly on YouTube holding what appear to be Glock firearms equipped with "Glock switches." For example, in a video posted to YouTube on August 13, 2021, **JONES** was depicted holding what appears to be a Glock firearm equipped with a "Glock switch" and a drum magazine (*see* Figure 4 below). **JONES** posted a photo of what appears to be the same firearm on his Instagram account on July 31, 2021 (*see* Figure 5 below).

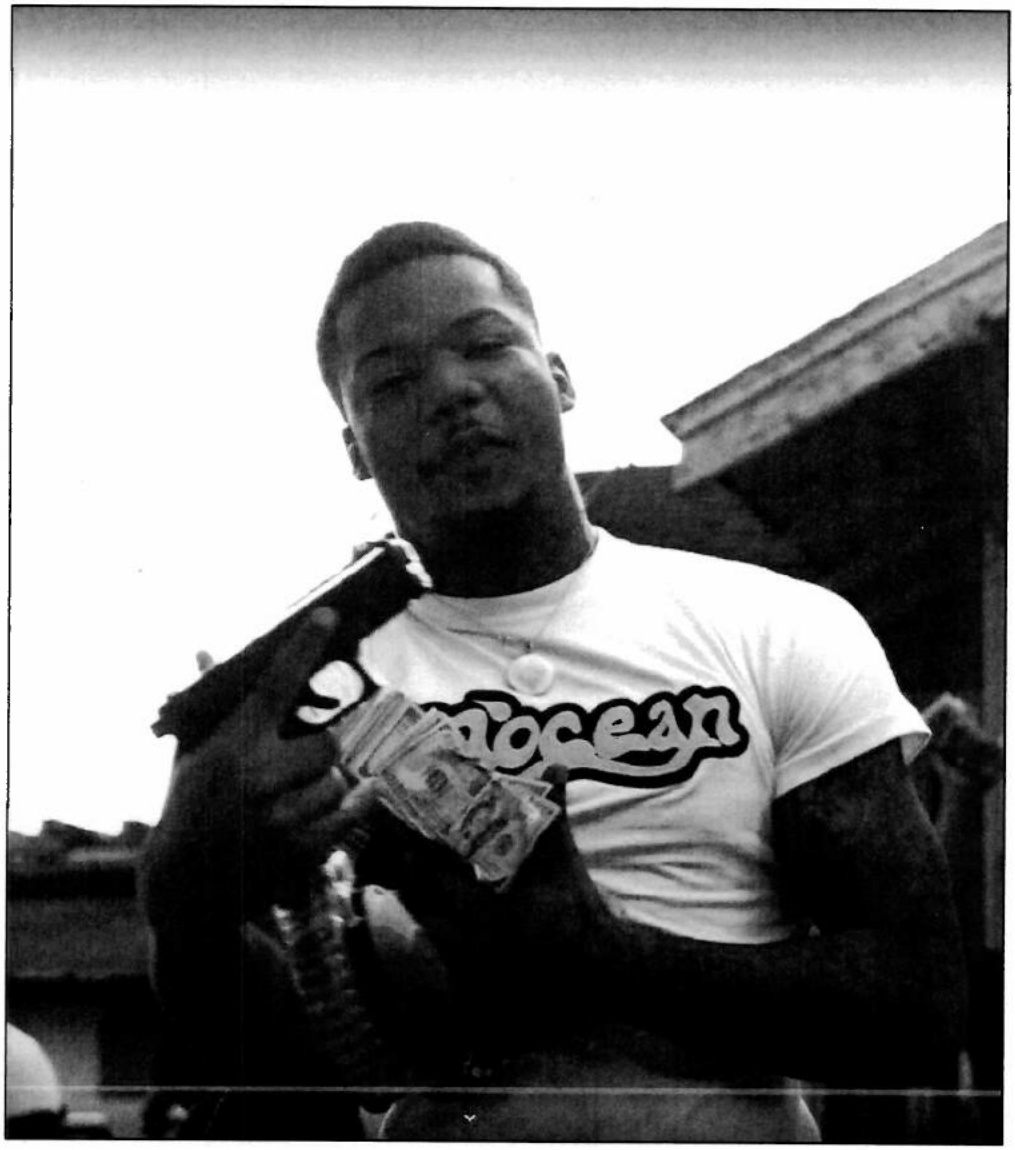

Fig. 4 (screenshot of rap video depicting **JONES** holding an apparent Glock firearm equipped with a "Glock switch" and a drum magazine, posted to YouTube on Aug. 13, 2021).

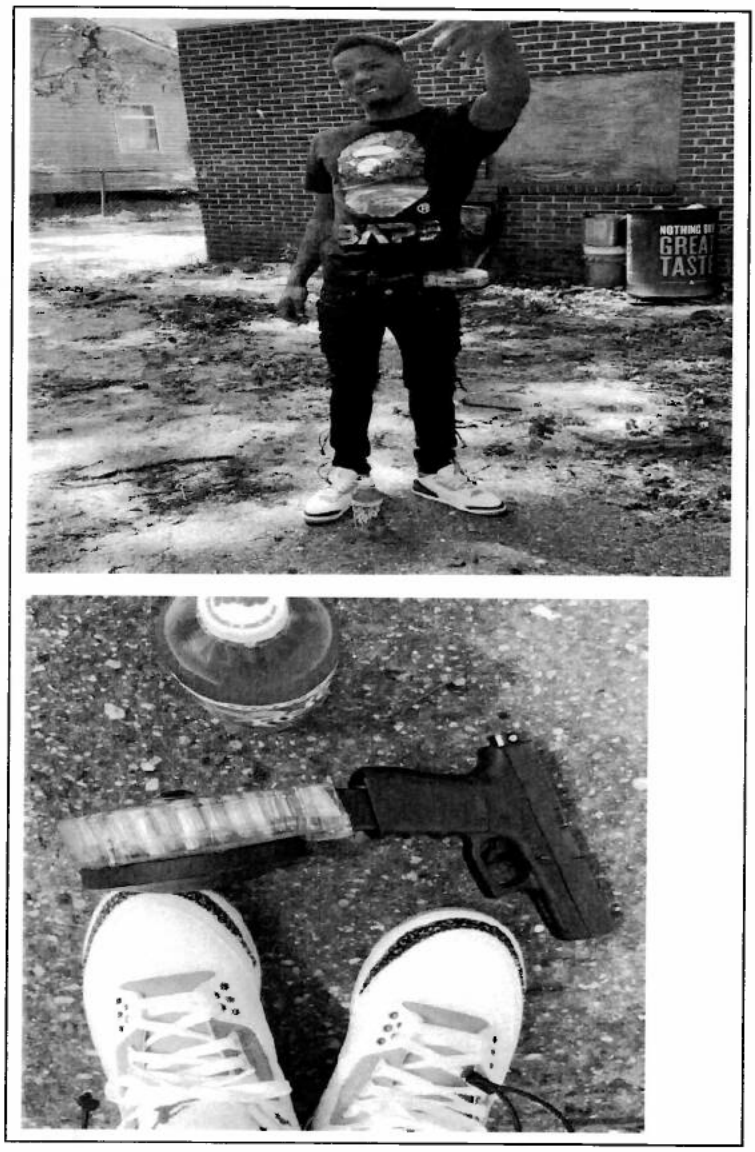

Fig. 5 (images depicting **JONES** holding an apparent Glock firearm equipped with a "Glock switch" and a drum magazine, posted to Instagram on July 31, 2021).

30. **JONES's** iPhone also contains several videos appearing to depict bulk marijuana with metadata dated between June 2022 and February 2023. For example, the phone contains a

video with metadata dated February 1, 2023—the same day as the search warrant at **JONES's** apartment—depicting apparent bulk marijuana (*see* Figure 6 below).

Fig. 6 (screenshot of video of apparent bulk marijuana, dated Feb. 1, 2023).

31. **JONES's** iPhone also contains an photo with metadata dated February 1, 2023—the same day as the search warrant at **JONES's** apartment—apparently depicting **JONES** holding a Glock firearm equipped with an extended magazine, which appears to be one of the firearms seized from **JONES's** apartment (*see* Figure 7 below). **JONES** has the tattoos reflected in the image.

Fig. 7 (image depicting **JONES** holding a Glock firearm similar to one seized from his apartment, dated February 1, 2023).

32. **JONES** is a multi-convicted felon, with several convictions from 2019 in the Mobile County Circuit Court for violent felonies including second-degree robbery, multiple second-degree assaults, and several convictions for shooting into occupied and unoccupied vehicles and dwellings. As a result of his felony convictions, **JONES** is prohibited from possessing firearms by federal law. DNA analysis of the Glock firearms seized from **JONES's** apartment concluded that there was "very strong support" for the proposition that **JONES** is a contributor to the DNA material collected from the firearms.

33. There are numerous other examples of similar evidence in the phones. Additionally, the phones contains several items of evidence tying the phones to **JONES** (*e.g.*, pictures of him and items containing his name). As noted above, the Apple IDs connected to **JONES** that are the subject of this warrant application are [redacted]**@icloud.com** and [redacted]**@icloud.com**. According to the data on the phones, the data may have never been backed up to iCloud.

BACKGROUND CONCERNING APPLE[1]

34. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

---

[1] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Manage and use your Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "Introduction to iCloud," available at https://support.apple.com/kb/PH26502; "What does iCloud back up?," available at

35. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a

---

https://support.apple.com/kb/PH12519; and "Apple Platform Security," available at https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf.

backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

36. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-

provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

37. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

38. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs"

for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

39. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

40. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud

can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

41. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

42. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

43. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-

location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

44. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

46. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

47. Based on the forgoing, I request that the Court issue the proposed search warrant.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Kimberly Anne Suhi
Senior Special Agent
Bureau of Alcohol, Tobacco, Firearms & Explosives

THE ABOVE AGENT HAS ATTESTED TO THIS AFFIDAVIT PURSUANT TO FED. R. CRIM. P. 4.1(b)(2)(B) THIS 19th DAY OF MAY 2023.

SONJA F. BIVINS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with [redacted]**@icloud.com** and [redacted]**@icloud.com** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

SEALED

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 21 U.S.C. § 846 (Conspiracy to Possess with Intent to Distribute Marijuana); 21 U.S.C. § 841(a)(1) (Possession with Intent to Distribute Marijuana); 18 U.S.C. § 924(c)(1)(A)(i) (Possession of Firearm in Furtherance of a Drug Trafficking Crime); 18 U.S.C. § 922(g)(1) (Possession of a Firearm by a Prohibited Person (Felon)); and 26 U.S.C. § 5861(d) (Possession of an Unregistered Firearm), those violations involving **Hassan Decalpton JONES** and occurring on or after July 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. Any and all records relating to the sale and/or possession of narcotics, the sale and/or possession of firearms, the sale and/or possession of machine gun conversion devices, the possession, use and whereabouts of proceeds from illegal activities, witness intimidation, and/or the identification of suppliers and customers from illegal activities;

b. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

e. The identity of the person(s) who communicated with the user ID about matters relating to firearms, narcotics, conversion devices, money laundering and/or witness intimidation, including records that help reveal their whereabouts.